## **GetLongPathName**

Carefully manage buffer sizes

Sean Barnum, Cigital, Inc. [vita<sup>1</sup>]

Copyright © 2007 Cigital, Inc.

2007-03-23

## Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 6179 bytes

• Indeterminate File/Path  • File Path Management  • winbase.h  The return buffer for GetLongPathName() and similar functions might return a truncated path and lead to hard-to-find errors.  The GetLongPathName() or GetShortPathName() function converts a path to its long or short form. If the IpszLongPath or IpszShortPath buffer is too small to contain the path, the return value is the size of the buffer, in TCHARs, required to hold the path Call the function again with the proper sized buffer to retrieve the data.  The ASCII versions of these functions limit paths to MAX_PATH characters, including the terminating NULL. Unicode versions can handle paths of up to over 32,000 characters if they begin with the specia notation "\\"\"\"\".  GetTempPath() returns the path to the directory for temporary files. It is subject to the same issue regarding potentially returning a path that is too large for the buffer.  APIS  Function Name Comments  GetLongPathName  GetLongPathNameA ASCII implementation  GetShortPathName  GetShortPathNameA ASCII implementation  GetShortPathNameA ASCII implementation  GetShortPathNameA ASCII implementation	Attack Category	<ul> <li>Path spoofing or confusion problem</li> </ul>		
Software Context  • File Path Management  • winbase.h  The return buffer for GetLongPathName() and similar functions might return a truncated path and lead to hard-to-find errors.  The GetLongPathName() or GetShortPathName() function converts a path to its long or short form. If the lpszLongPath or lpszShortPath buffer is too small to contain the path, the return value is the size of the buffer, in TCHARs, required to hold the path Call the function again with the proper sized buffer to retrieve the data.  The ASCII versions of these functions limit paths to MAX_PATH characters, including the terminating NULL. Unicode versions can handle paths of up to over 32,000 characters if they begin with the specia notation "\\?\?\".  GetTempPath() returns the path to the directory for temporary files. It is subject to the same issue regarding potentially returning a path that is too large for the buffer.  APIS  Function Name   Comments   GetLongPathName   GetLongPathName   GetLongPathName   GetLongPathName   GetShortPathName   GetShortPathName   ASCII implementation   GetShortPathName   Unicode implementation	Vulnerability Category	Buffer Management		
Location  • winbase.h  The return buffer for GetLongPathName() and similar functions might return a truncated path and lead to hard-to-find errors.  The GetLongPathName() or GetShortPathName() function converts a path to its long or short form. If the lpszLongPath or lpszShortPath buffer is too small to contain the path, the return value is the size of the buffer, in TCHARs, required to hold the path Call the function again with the proper sized buffer to retrieve the data.  The ASCII versions of these functions limit paths to MAX_PATH characters, including the terminating NULL. Unicode versions can handle paths of up to over 32,000 characters if they begin with the specia notation "\\?\?\".  GetTempPath() returns the path to the directory for temporary files. It is subject to the same issue regarding potentially returning a path that is too large for the buffer.  APIS  Function Name Comments  GetLongPathName  GetLongPathNameA ASCII implementation  GetShortPathNameW Unicode implementation  GetShortPathNameA ASCII implementation  GetShortPathNameA Unicode implementation		Indeterminate File/Path		
The return buffer for GetLongPathName() and similar functions might return a truncated path and lead to hard-to-find errors.  The GetLongPathName() or GetShortPathName() function converts a path to its long or short form. If the lpszLongPath or lpszShortPath buffer is too small to contain the path, the return value is the size of the buffer, in TCHARs, required to hold the path Call the function again with the proper sized buffer to retrieve the data.  The ASCII versions of these functions limit paths to MAX_PATH characters, including the terminating NULL. Unicode versions can handle paths of up to over 32,000 characters if they begin with the specia notation "\\?\\".\".  GetTempPath() returns the path to the directory for temporary files. It is subject to the same issue regarding potentially returning a path that is too large for the buffer.  APIS  Function Name Comments  GetLongPathName  GetLongPathNameA ASCII implementation  GetShortPathNameW Unicode implementation  GetShortPathNameA ASCII implementation  GetShortPathNameA ASCII implementation	Software Context	File Path Management		
similar functions might return a truncated path and lead to hard-to-find errors.  The GetLongPathName() or GetShortPathName() function converts a path to its long or short form. If the lpszLongPath or lpszShortPath buffer is too small to contain the path, the return value is the size of the buffer, in TCHARs, required to hold the path Call the function again with the proper sized buffer to retrieve the data.  The ASCII versions of these functions limit paths to MAX_PATH characters, including the terminating NULL. Unicode versions can handle paths of up to over 32,000 characters if they begin with the special notation "\\?\\?\".  GetTempPath() returns the path to the directory for temporary files. It is subject to the same issue regarding potentially returning a path that is too large for the buffer.  APIS  Function Name Comments  GetLongPathName  GetLongPathNameA ASCII implementation  GetShortPathNameA ASCII implementation  GetShortPathNameA ASCII implementation	Location	• winbase.h		
function converts a path to its long or short form. If the lpszLongPath or lpszShortPath buffer is too small to contain the path, the return value is the size of the buffer, in TCHARs, required to hold the path Call the function again with the proper sized buffer to retrieve the data.  The ASCII versions of these functions limit paths to MAX_PATH characters, including the terminating NULL. Unicode versions can handle paths of up to over 32,000 characters if they begin with the special notation "\\?\".  GetTempPath() returns the path to the directory for temporary files. It is subject to the same issue regarding potentially returning a path that is too large for the buffer.  APIS  Function Name  GetLongPathName  GetLongPathName  GetLongPathNameA  ASCII implementation  GetShortPathNameA  GetShortPathNameA  GetShortPathNameA  GetShortPathNameA  GetShortPathNameA  Unicode implementation	Description	similar functions might return a truncated path and		
MAX_PATH characters, including the terminating NULL. Unicode versions can handle paths of up to over 32,000 characters if they begin with the special notation "\\?\".  GetTempPath() returns the path to the directory for temporary files. It is subject to the same issue regarding potentially returning a path that is too large for the buffer.  APIS  Function Name Comments  GetLongPathName  GetLongPathName  GetLongPathNameW Unicode implementation  GetShortPathNameA ASCII implementation  GetShortPathNameA ASCII implementation  GetShortPathNameA Unicode implementation  GetShortPathNameW Unicode implementation		function converts a path to its long or short form. If the lpszLongPath or lpszShortPath buffer is too small to contain the path, the return value is the size of the buffer, in TCHARs, required to hold the path Call the function again with the proper sized buffer		
for temporary files. It is subject to the same issue regarding potentially returning a path that is too large for the buffer.  Function Name		MAX_PATH characters, including the terminating NULL. Unicode versions can handle paths of up to over 32,000 characters if they begin with the special		
GetLongPathName  GetLongPathNameA  GetLongPathNameW  Unicode implementation  GetShortPathName  GetShortPathNameA  ASCII implementation  GetShortPathNameA  Unicode implementation  Unicode implementation		for temporary files. It is subject to the same issue regarding potentially returning a path that is too		
GetLongPathNameA ASCII implementation GetLongPathNameW Unicode implementation GetShortPathName GetShortPathNameA ASCII implementation GetShortPathNameW Unicode implementation	APIs	Function Name Comments		
GetShortPathName Unicode implementation  GetShortPathName ASCII implementation  GetShortPathNameW Unicode implementation		GetLongPathName		
GetShortPathName  GetShortPathNameA ASCII implementation  GetShortPathNameW Unicode implementation		GetLongPathNameA ASCII implementation		
GetShortPathNameA ASCII implementation GetShortPathNameW Unicode implementation		GetLongPathNameW Unicode implementation		
GetShortPathNameW Unicode implementation		GetShortPathName		
GetShortPathNameW Unicode implementation		GetShortPathNameA ASCII implementation		
A				
		GetTempPath		

1

GetLongPathName
ID: 753-BSI | Version: 4 | Date: 5/16/08 2:39:23 PM

<sup>1.</sup> http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

	GetTempPathA			ASCII Implementation		
	GetTempPathW			de implementation		
Method of Attack			'			
Exception Criteria						
Solutions	Solution Applicability			Solution Efficacy		
	When any of the indicated functions are called.	It is a be practice always a path but MAX_F characted ASCII uthis gual buffers alarge en However Unicode with son function may not be suffice So shou also che confirm the size sufficien. For the function issue, if return v is greated the buff cchBuff the function again which buffer the function again which is the suffice model the suffice en hold the suffice sufficient to the suffice sufficient to the suffice s	to size effers to PATH ers. For usage, rantees will be ough. er, for e usage, me as this always cient. Id eck to that was nt.  In a sat the alue er than er size, er, call ction ith a hat is ough to path.	Effective.		
Signature Details	LPCTSTR lpszS LPTSTR lpszLo DWORD cchBu ); DWORD GetSh LPCTSTR lpszL LPTSTR lpszSh DWORD cchBu );	DWORD GetShortPathName( LPCTSTR lpszLongPath, LPTSTR lpszShortPath, DWORD cchBuffer				

	DWORD nBufferLength,	,		
	LPTSTR lpBuffer );			
Examples of Incorrect Code	TCHAR shortPath[MAX_PATH] = TEXT("C:\\ADIR\\SHORT~1.TXT"); LPCTSTR lpszShortPath = shortPath; DWORD buffSize = 15; // Buffer is too small LPTSTR lpszLongPath = (LPTSTR)malloc(buffSize *sizeof(TCHAR)); DWORD result = GetLongPath(shortPath, longPath, buffSize); /* Might have failed - potential bug if don't check result */  TCHAR shortPath[MAX_PATH] = TEXT("C:\\ADIR\\SHORT~1.TXT"); LPCTSTR lpszShortPath = shortPath; DWORD buffSize = MAX_PATH; LPTSTR lpszLongPath = (LPTSTR)malloc(buffSize *sizeof(TCHAR)); DWORD result = GetLongPath(shortPath, longPath, buffSize); if (result > MAX_PATH) { delete lpszLongPath; buffSize = result; lpszLongPath = (LPTSTR)malloc(buffSize*sizeof(TCHAR)) if (! GetLongPath(shortPath, longPath, buffSize)) { handleError(); }			
Examples of Corrected Code				
Source Reference	default.asp?url=/libr	http://msdn.microsoft.com/library/ default.asp?url=/library/en-us/fileio/fs/ getlongpathname.asp <sup>2</sup>		
Recommended Resources	MSDN reference for	MSDN reference for GetShortPathName <sup>4</sup>		
Discriminant Set	<b>Operating System</b>	• Windows		
	Languages	• C • C++		

## Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about "Fair Use," contact Cigital at copyright@cigital.com<sup>1</sup>.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

<sup>1.</sup> mailto:copyright@cigital.com